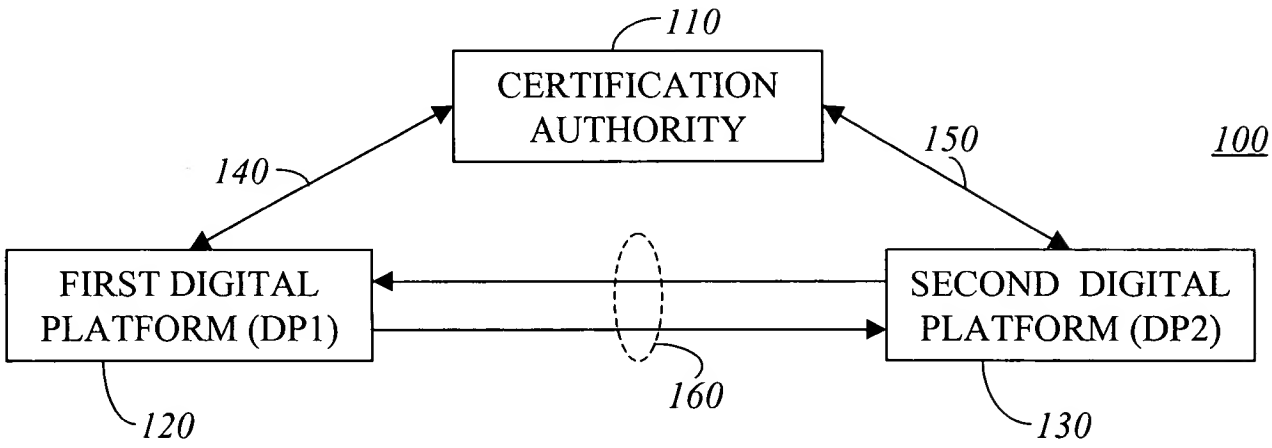

Figure 1

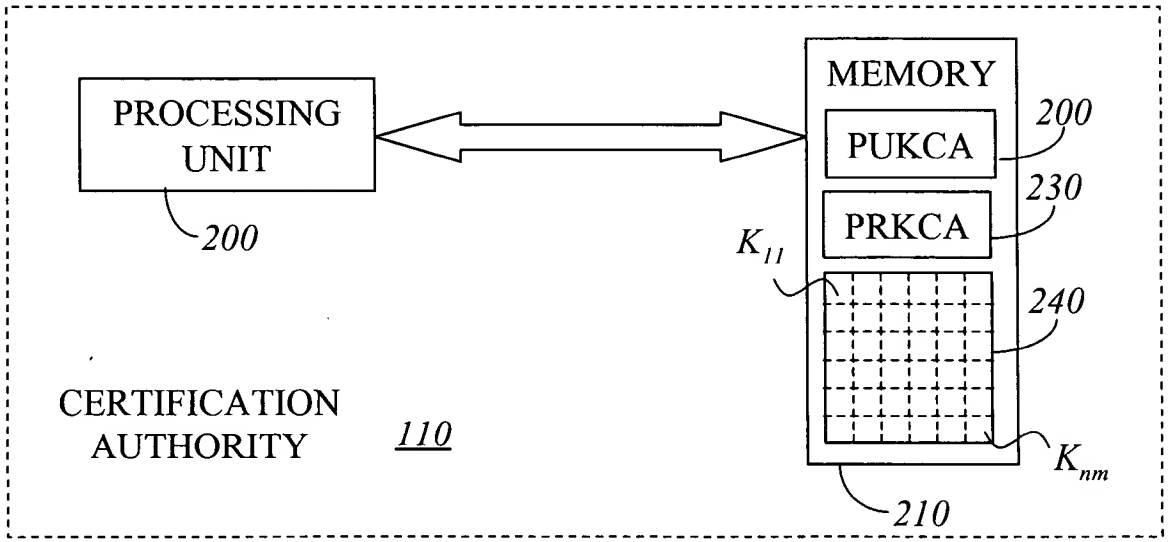

Figure 2

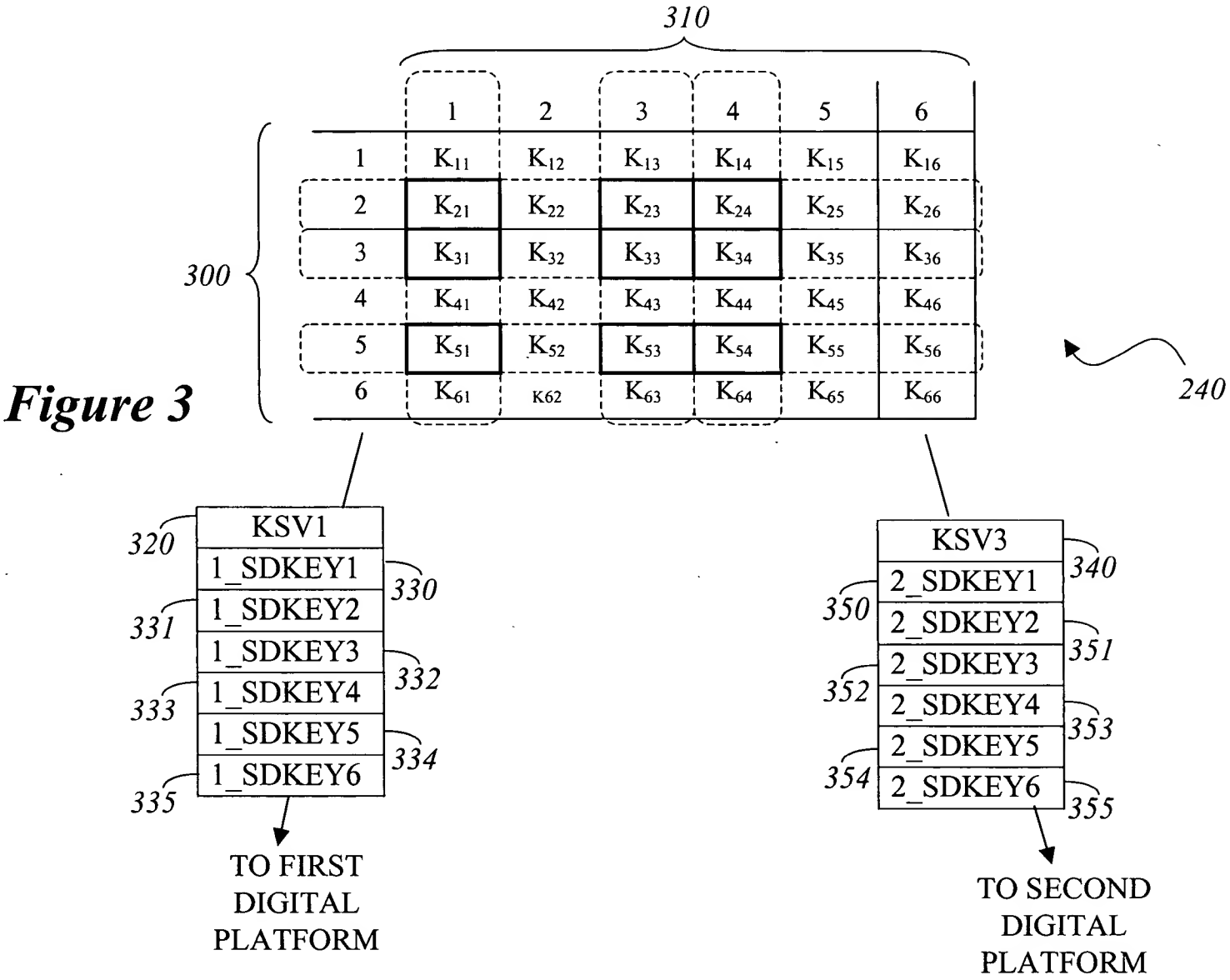
310
1
2
3
4
5
6
1 K11 K12 K13 K14 K15 K16
2 K21 K22 K23 K24 K25 K26
3 K31 K32 K33 K34 K35 K36
4 K41 K42 K43 K44 K45 K46
5 K51 K52 K53 K54 K55 K56
6 K61 K62 K63 K64 K65 K66
300
240
KSV1
1_SDKEY1
1_SDKEY2
1_SDKEY3
1_SDKEY4
1_SDKEY5
1_SDKEY6
320
330
331
332
333
334
335
TO FIRST DIGITAL PLATFORM
KSV3
2_SDKEY1
2_SDKEY2
2_SDKEY3
2_SDKEY4
2_SDKEY5
2_SDKEY6
340
350
351
352
353
354
355
TO SECOND DIGITAL PLATFORM

Figure 3

	SELECT DEVICE KEYS (DP1)	CONTENTS
330		
331	1_SDKEY1	$K_{21} + K_{31} + K_{51}$
332	1_SDKEY2	$K_{22} + K_{32} + K_{52}$
333	1_SDKEY3	$K_{23} + K_{33} + K_{53}$
334	1_SDKEY4	$K_{24} + K_{34} + K_{54}$
335	1_SDKEY5	$K_{25} + K_{35} + K_{55}$
	1_SDKEY6	$K_{26} + K_{36} + K_{56}$

Figure 4

	SECRET DEVICE KEYS (DP2)	CONTENTS
350		
351	2_SDKEY1	$K_{11} + K_{13} + K_{14}$
352	2_SDKEY2	$K_{21} + K_{23} + K_{24}$
353	2_SDKEY3	$K_{31} + K_{33} + K_{34}$
354	2_SDKEY4	$K_{41} + K_{43} + K_{44}$
355	2_SDKEY5	$K_{51} + K_{53} + K_{54}$
	2_SDKEY6	$K_{61} + K_{63} + K_{64}$

Figure 5

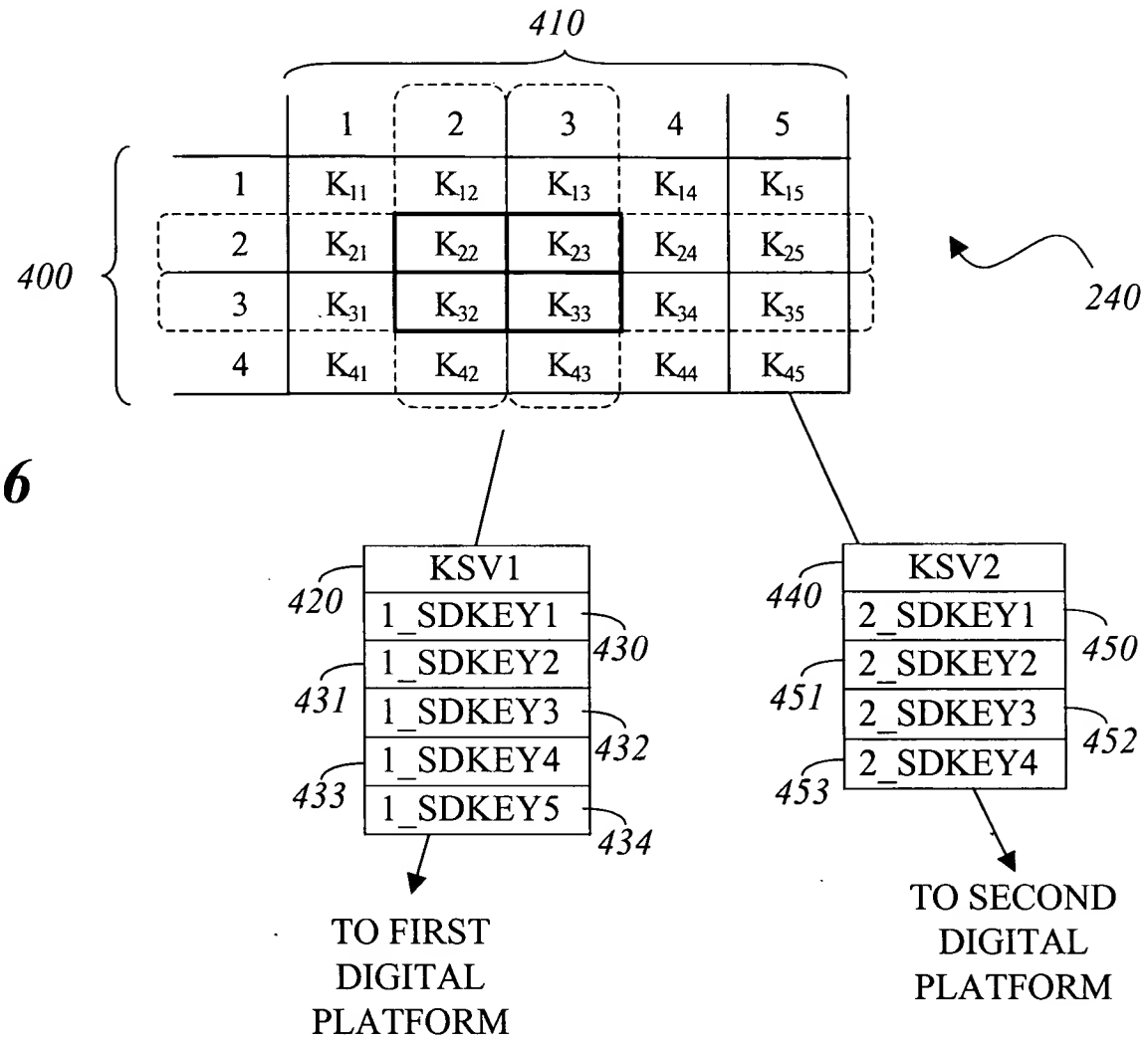
410
400
1
2
3
4
5
1
2
3
4
K11
K12
K13
K14
K15
K21
K22
K23
K24
K25
K31
K32
K33
K34
K35
K41
K42
K43
K44
K45
240
KSV1
420
1_SDKEY1
430
1_SDKEY2
431
1_SDKEY3
432
1_SDKEY4
433
1_SDKEY5
434
TO FIRST DIGITAL PLATFORM
KSV2
440
2_SDKEY1
450
2_SDKEY2
451
2_SDKEY3
452
2_SDKEY4
453
TO SECOND DIGITAL PLATFORM

Figure 6

	SECRET DEVICE KEYS (DP1)	CONTENTS
430		
431	1_SDKEY1	$K_{21} + K_{31}$
432	1_SDKEY2	$K_{22} + K_{32}$
433	1_SDKEY3	$K_{23} + K_{33}$
434	1_SDKEY4	$K_{24} + K_{34}$
	1_SDKEY5	$K_{25} + K_{35}$

Figure 7

	SECRET DEVICE KEYS (DP2)	CONTENTS
450		
451	2_SDKEY1	$K_{12} + K_{13}$
452	2_SDKEY2	$K_{22} + K_{23}$
453	2_SDKEY3	$K_{32} + K_{33}$
	2_SDKEY4	$K_{42} + K_{43}$

Figure 8

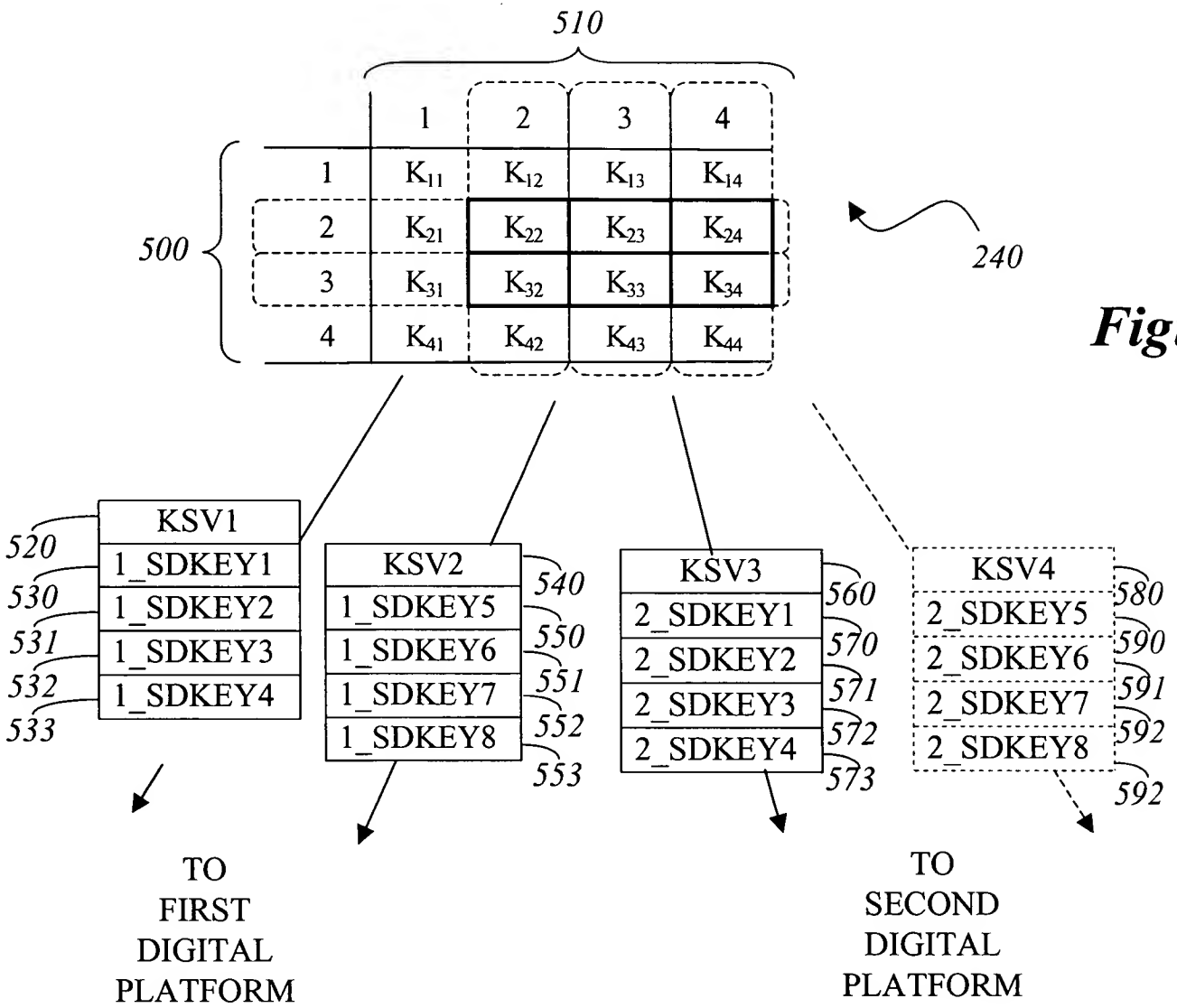

Figure 9

	SECRET DEVICE KEYS (DP1)	CONTENTS
530		
531	1_SDKEY1	$K_{21} + K_{31}$
532	1_SDKEY2	$K_{22} + K_{32}$
533	1_SDKEY3	$K_{23} + K_{33}$
	1_SDKEY4	$K_{24} + K_{34}$

Figure 10

	SECRET DEVICE KEYS (DP2)	CONTENTS
550		
551	1_SDKEY5	$K_{12} + K_{14}$
552	1_SDKEY6	$K_{22} + K_{24}$
553	1_SDKEY7	$K_{32} + K_{34}$
	1_SDKEY8	$K_{42} + K_{44}$

Figure 11

	SECRET DEVICE KEYS (DP1)	CONTENTS
570		
571	2_SDKEY1	$K_{12} + K_{13}$
572	2_SDKEY2	$K_{22} + K_{23}$
573	2_SDKEY3	$K_{32} + K_{33}$
	2_SDKEY4	$K_{42} + K_{43}$

Figure 12

	SECRET DEVICE KEYS (DP2)	CONTENTS
590		
591	2_SDKEY5	$K_{21} + K_{31}$
592	2_SDKEY6	$K_{22} + K_{32}$
593	2_SDKEY7	$K_{23} + K_{33}$
	2_SDKEY8	$K_{24} + K_{34}$

Figure 13

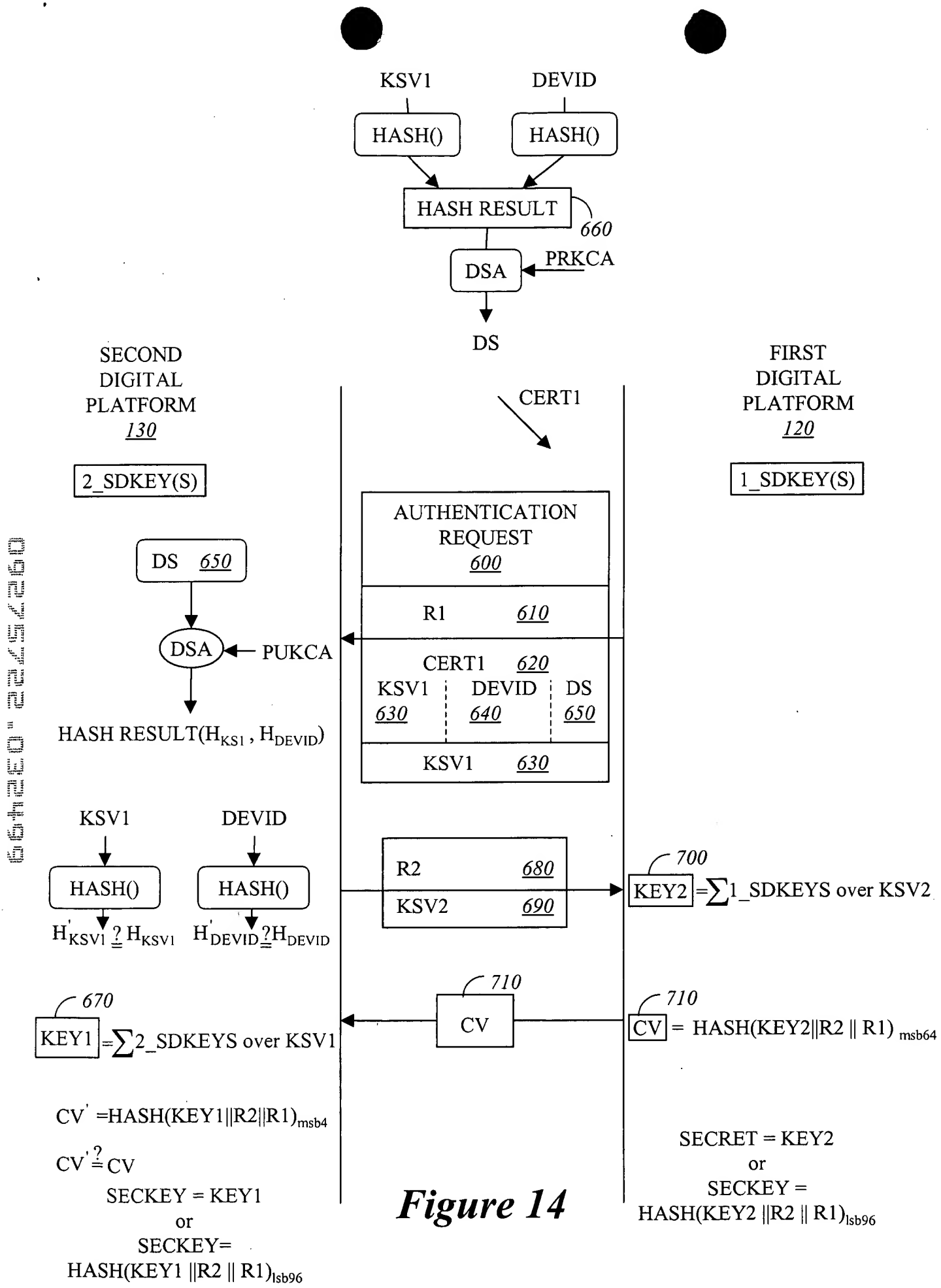
KSV1
DEVID
HASH()
HASH()
HASH RESULT
660
DSA
PRKCA
DS
SECOND DIGITAL PLATFORM 130
FIRST DIGITAL PLATFORM 120
CERT1
2_SDKEY(S)
1_SDKEY(S)
AUTHENTICATION REQUEST 600
R1 610
CERT1 620
KSV1 630
DEVID 640
DS 650
KSV1 630
DS 650
DSA
PUKCA
HASH RESULT(H_{KS1} , H_{DEVID})
KSV1
DEVID
HASH()
HASH()
$H'_{KSV1} \stackrel{?}{=} H_{KSV1}$
$H'_{DEVID} \stackrel{?}{=} H_{DEVID}$
R2 680
KSV2 690
700
KEY2 $=\sum$1_SDKEYS over KSV2
710
CV
710
CV = HASH(KEY2||R2 || R1) msb64
670
KEY1 $=\sum$2_SDKEYS over KSV1
$CV' = HASH(KEY1||R2||R1)_{msb4}$
$CV' \stackrel{?}{=} CV$
SECKEY = KEY1
or
SECKEY= HASH(KEY1 ||R2 || R1)lsb96
SECRET = KEY2
or
SECKEY = HASH(KEY2 ||R2 || R1)lsb96

Figure 14

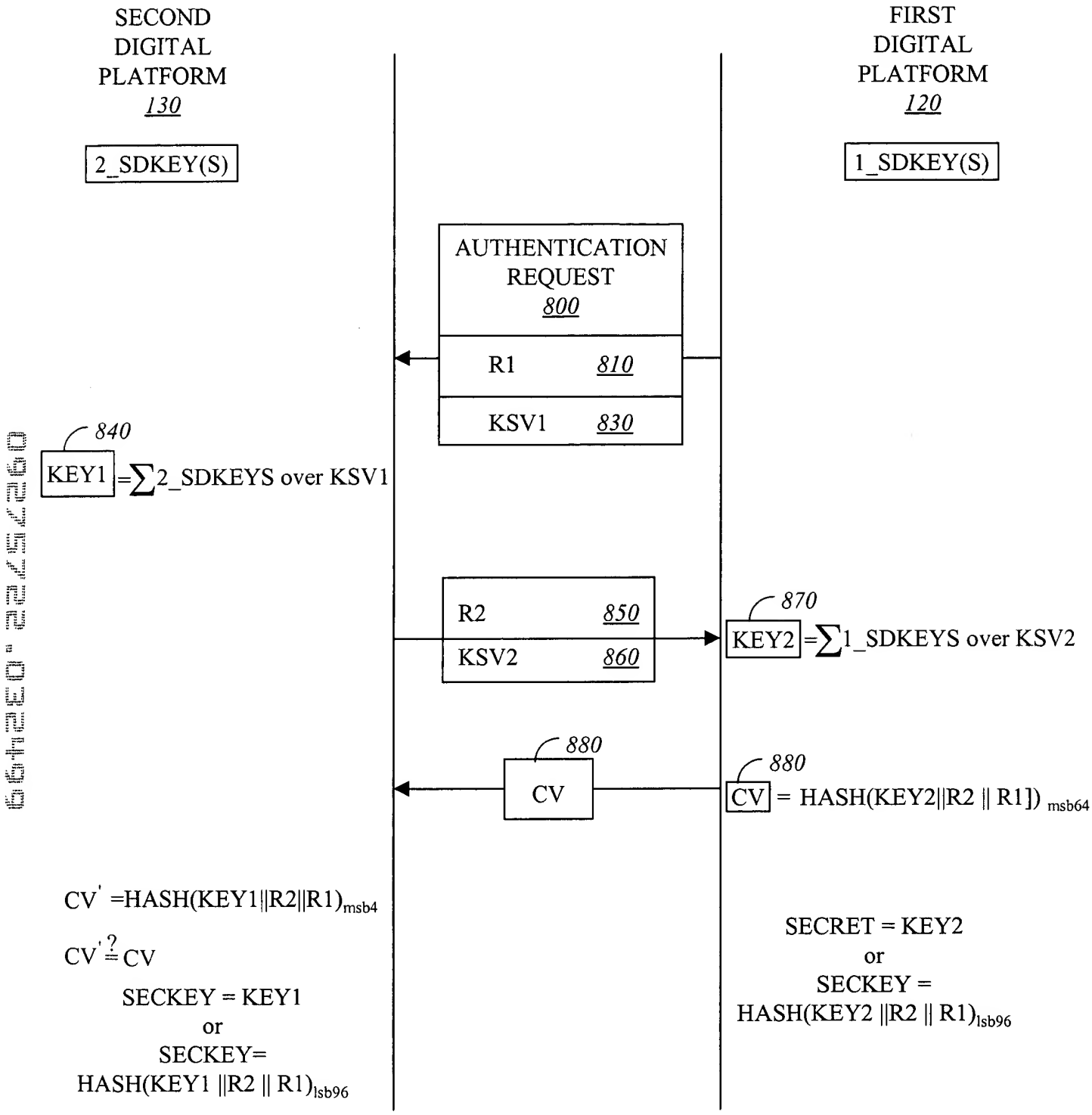
SECOND DIGITAL PLATFORM 130
2_SDKEY(S)
FIRST DIGITAL PLATFORM 120
1_SDKEY(S)
AUTHENTICATION REQUEST 800
R1 810
KSV1 830
840
KEY1 =∑2_SDKEYS over KSV1
R2 850
KSV2 860
870
KEY2 =∑1_SDKEYS over KSV2
880
CV
880
CV = HASH(KEY2||R2 || R1]) msb64
CV' =HASH(KEY1||R2||R1)msb4
CV' ? CV
SECKEY = KEY1
or
SECKEY=
HASH(KEY1 ||R2 || R1)lsb96
SECRET = KEY2
or
SECKEY =
HASH(KEY2 ||R2 || R1)lsb96

Figure 15